

May 2005

INFORMATION SECURITY

Radio Frequency Identification Technology in the Federal Government



G A O

Accountability ★ Integrity ★ Reliability

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE MAY 2005		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Information Security: Radio Frequency Identification Technology in the Federal Government				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Government Accountability Office 441 G St., NW Washington, DC 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 41	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Highlights of [GAO-05-551](#), a report to congressional requesters

Why GAO Did This Study

Radio frequency identification (RFID) is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag that is attached to or embedded in an object, such as a product, case, or pallet. Federal agencies have begun implementation of RFID technology, which offers them new capabilities and efficiencies in operations. The reduced cost of the technology has made the wide-scale use of it a real possibility for government and industry organizations.

Accordingly, GAO was requested to discuss considerations surrounding RFID technology implementation in the federal government. Specifically, GAO was asked to (1) provide an overview of the technology; (2) identify the major initiatives at federal agencies that use or propose to use the technology; (3) discuss the current standards, including those for interoperability, that exist; (4) discuss potential legal issues that the 24 Chief Financial Officer (CFO) Act agencies have identified in their planning for technology implementation; and (5) discuss security and privacy considerations surrounding the technology and the tools and practices available to mitigate them. The Office of Management and Budget agreed with the contents of this report.

www.gao.gov/cgi-bin/getrpt?GAO-05-551.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov.

INFORMATION SECURITY

Radio Frequency Identification Technology in the Federal Government

What GAO Found

The main technology components of an RFID system are a tag, reader, and database. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag (see figure).

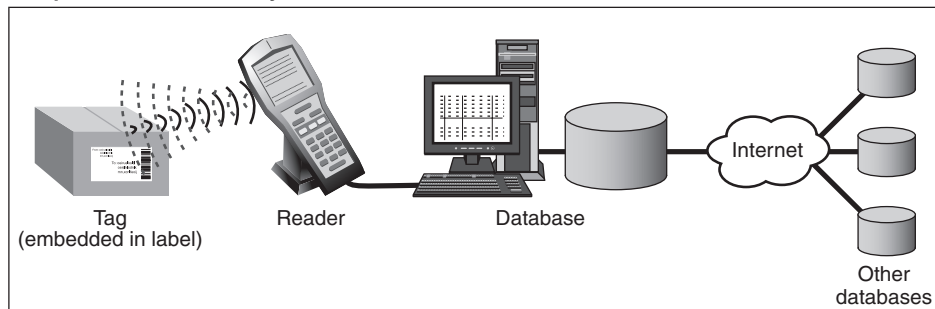
The major initiatives at federal agencies that use or propose to use the technology include physical access control and tracking assets, documents, or materials. For example, the Department of Homeland Security is using it to track and identify assets, weapons, and baggage on flights.

RFID standards define a set of rules, conditions, or requirements that the components of the system must meet in order to operate effectively. There are multiple sets of standards that guide the use of RFID technology. In addition, the standards used often depend on the type of activity the application is used for and the industry or country in which it is used. For applications where global interoperability between systems is necessary, such as electronic passports or global supply chains, a common set of standards can assist with the proper interaction and interchange of information between systems.

Of the 16 agencies that responded to the question on legal issues associated with RFID implementation in our survey, only one identified what it considered to be legal issues. These issues relate to protecting an individual's right to privacy and tracking sensitive documents and evidence.

The use of tags and databases raises important security considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Key privacy concerns include tracking an individual's movements and profiling an individual's habits, among others. Tools and practices are available to address these considerations, including existing and proposed information security technologies and practices, and other practices required by law.

Components of an RFID System



Source: GAO.

Contents

Letter		1
	Results in Brief	2
	Background	4
	RFID Technology Overview	4
	Several Agencies Have Begun Implementation of RFID Systems	12
	Multiple Sets of Standards Guide RFID Technology	14
	Federal Agencies Raise Few Legal Issues	17
	Security and Privacy Considerations with RFID	18
	Summary	27
	Agency Comments	27

Appendixes		
	Appendix I: Objectives, Scope, and Methodology	29
	Appendix II: Research and Development Efforts Are Under Way	31
	Appendix III: Illustrative List of Standards-Setting Organizations for RFID Systems	33
	Appendix IV: Illustrative List of Standards for RFID Systems	35
	Appendix V: Staff Acknowledgments	36

Tables	Table 1: Typical Characteristics of RFID Tags	8
	Table 2: Common RFID Operating Frequencies for Passive Tags	11
	Table 3: Federal Agencies' Reported Use or Planned Use of RFID Technology	13

Figures	Figure 1: Main Components of an RFID System	5
	Figure 2: An Example of the Back of an RFID Tag	6
	Figure 3: The Reader	8
	Figure 4: The Database	9

Abbreviations

ANSI	American National Standards Institute
CFO	Chief Financial Officer
DOD	Department of Defense
EPA	Environmental Protection Agency
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NTIA	National Telecommunications and Information Administration
OFEE	Office of the Federal Environmental Executive
RFID	radio frequency identification
UHF	ultrahigh frequency

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

May 27, 2005

The Honorable Christopher Cox
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Zoe Lofgren
Committee on Homeland Security
House of Representatives

The Honorable Mac Thornberry
House of Representatives

Radio frequency identification (RFID) is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The tag can be attached to or embedded in the object to be identified, such as a product, case, or pallet. RFID provides identification and tracking capabilities by using wireless communication to transmit data.

The technology can provide a more efficient method for federal agencies, manufacturers, retailers, and suppliers to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls, among other functions, by providing real-time access to information. The use of this technology also has the potential to assist agencies in tracking their assets, thereby maintaining more accurate inventory records.

In response to your request, our report discusses considerations surrounding RFID technology implementation in the federal government. Specifically, our objectives were to (1) provide an overview of the technology, with an emphasis on passive technology; (2) identify the major initiatives at federal agencies that use or propose to use the technology; (3) discuss the current standards, including those for interoperability, that exist; (4) discuss potential legal issues that the 24 Chief Financial Officer

(CFO) Act of 1990¹ agencies have identified in their planning for technology implementation; and (5) discuss security and privacy considerations surrounding the technology and the tools and practices available to mitigate them.

We surveyed 23 of the 24 CFO Act agencies to gather information on whether the agencies are incorporating the technology into their systems, what they are using the technology for, and any security, privacy, or legal issues.² Appendix I contains a description of our objectives, scope, and methodology. We performed our review in Washington, D.C., from September 2004 through April 2005 in accordance with generally accepted government auditing standards.

Results in Brief

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The main technology components of an RFID system are a tag, reader, and database. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. Passive tags do not contain their own power source, such as a battery. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government and industry organizations.

The major initiatives at federal agencies that use or propose to use the technology include physical access control and tracking assets, documents, or materials. Thirteen of the 24 CFO Act agencies reported having implemented or having a specific plan to implement the technology in one or more applications. For example, the Department of Homeland Security is using it to track and identify assets, weapons, and baggage on flights. The Department of Defense (DOD) is also using it to track shipments.

RFID standards define a set of rules, conditions, or requirements that the components of a system (i.e., tag, reader, and database) must meet in order to operate effectively, ensure that tags meet intended designs, provide adequate protection of data for both security and privacy issues, and define

¹31 U.S.C. § 901.

²The Department of Defense (DOD) was not issued a survey because we collected relevant data through other ongoing work.

coding information contained on the tags. Multiple sets of standards guide the implementation and use of RFID technology. Additionally, multiple standards-setting organizations are involved in the development of standards. The standards used often depend on the type of activity the application is used for and the industry or country in which it is used. For applications where global interoperability between systems is necessary, such as electronic passports or global supply chains, a common set of standards can govern the interaction and interchange of information between systems.

Of the 16 agencies that responded to the question on legal issues associated with RFID implementation in our survey, only one identified what it considered to be legal issues. These issues relate to protecting an individual's right to privacy and tracking sensitive documents and evidence.

Several security and privacy issues are associated with federal and commercial use of RFID technology. The security of tags and databases raises important considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Tools and practices to address these security issues, such as compliance with the risk-based framework mandated by the Federal Information Security Management Act (FISMA) of 2002³ and employing encryption and authentication technologies, can help agencies achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing secondary uses of information. The Privacy Act of 1974 limits federal agencies' use and disclosure of personal information,⁴ and the privacy impact assessments required by the E-Government Act of 2002 provide an existing framework for agencies to follow in assessing the impact on privacy when implementing RFID technology.⁵ Additional measures proposed to mitigate privacy issues, such as using a deactivation mechanism on the tag, incorporating blocking technology to disrupt transmission, and implementing an opt-in/opt-out framework for consumers remain largely prospective.

³44 U.S.C. § 3544 (b).

⁴5 U.S.C. § 552 a(a)(4).

⁵44 U.S.C. § 3501 note. See Office of Management and Budget M-03-22, Sept. 26, 2003.

Office of Management and Budget officials stated that they agreed with the contents of the report and provided technical comments that we addressed in the report, as appropriate.

Background

RFID technology uses wireless communication in radio frequency bands to transmit data from tags to readers. A tag can be attached to or embedded in an object to be identified, such as a product, case, or pallet. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. For example, tags can be placed on car windshields so that toll systems can quickly identify and collect toll payments on roadways.

Interest in RFID technology began during World War II and has increased in the past few years. During the war, radio waves were used to determine whether approaching planes belonged to allies or enemies. Since then, exploration in radio technology research and development in commercial activities continued through the 1960s and evolved into marked advancements in the 1970s by companies, academic institutions, and the U.S. government. For example, at the request of the Department of Energy, Los Alamos National Laboratory developed a system to track nuclear materials by placing a tag in a truck and readers at the gates of secure facilities. This is the system used today in automated toll payment systems.

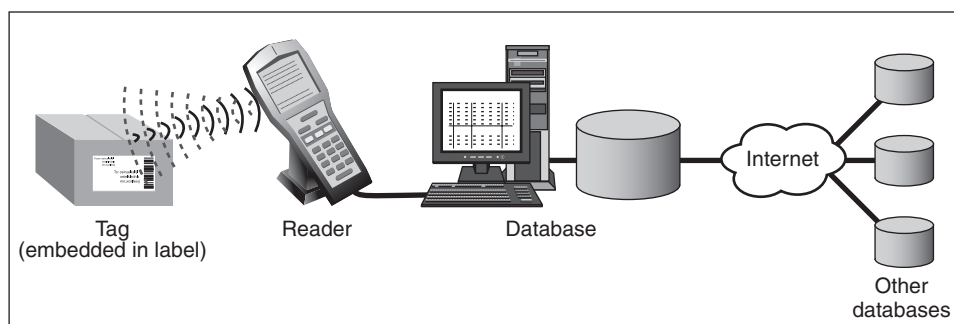
The technology offers several improvements over its predecessor technologies, such as barcodes and magnetic stripe cards. For instance, a tag can carry more data than a barcode or magnetic stripe and can be reprogrammed with new information if necessary. Additionally, tags do not typically require a line of sight to be read, as barcodes do, and can be read more rapidly and over greater distances. Mandates by large retailers and DOD requiring their top suppliers to use RFID tags, along with technological advancements and decreased costs, have spurred the proliferation of this technology. RFID technology is now being used in a variety of public and private-sector settings, ranging from tracking books in libraries to authenticating a key in order to start a vehicle.

RFID Technology Overview

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag.

The main technology components of an RFID system are the tag, reader, and database. (See fig. 1.)

Figure 1: Main Components of an RFID System

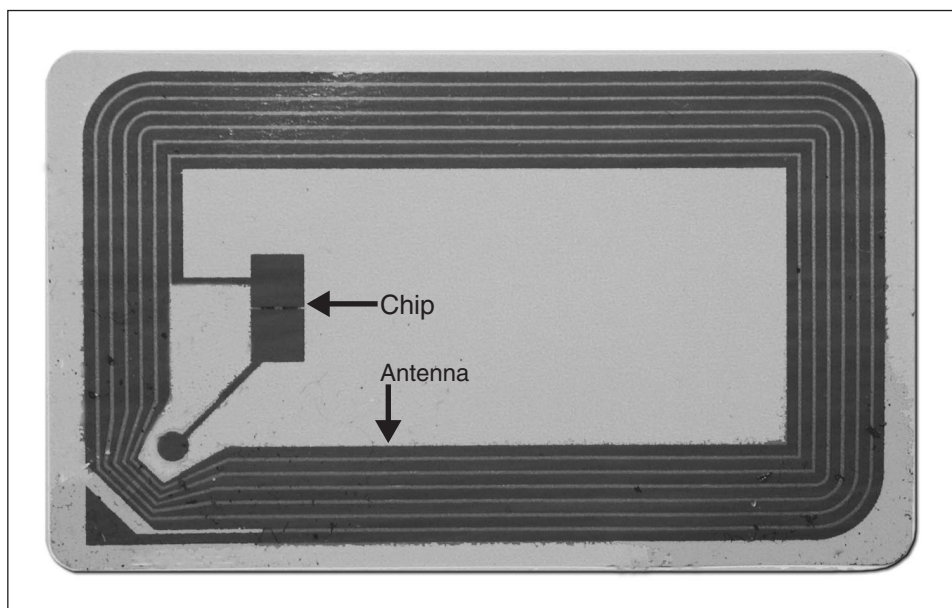


Source: GAO.

The Tag

An RFID tag, or transponder, consists of a chip and an antenna (see fig. 2). A chip can store a unique serial number or other information based on the tag's type of memory, which can be read-only, read-write, or write-once read-many. The antenna, which is attached to the microchip, transmits information from the chip to the reader. Typically, a larger antenna indicates a longer read range. The tag is attached to or embedded in an object to be identified, such as a product, case, or pallet, and can be scanned by mobile or stationary readers using radio waves. Figure 2 illustrates the back of an RFID tag that is used in libraries to track books.

Figure 2: An Example of the Back of an RFID Tag



Source: GAO.

The simplest version of a tag is a **passive tag**. Passive tags do not contain their own power source, such as a battery, nor can they initiate communication with a reader. Instead, the tag responds to the reader's radio frequency⁶ emissions and derives its power from the energy waves transmitted by the reader. A passive tag contains, at a minimum, a unique identifier for the individual item attached to the tag. Depending on the storage capacity of the tag, additional data can be added. Under perfect conditions, the tags can be read⁷ from a range of about 10 to 20 feet.⁸ The cost of passive tags ranges from 20 cents to several dollars. Costs vary based on the radio frequency used, amount of memory, design of the

⁶Frequency is the number of radio waves that pass a given point during a fixed period of time (e.g., the number of complete oscillations per second of energy).

⁷The read range of a tag is based on the size of the antenna, frequency used, power of the reader, and the material between the tag and reader.

⁸Although these tags can theoretically be read at 30 feet, when factoring in circumstances that can interfere with the read range (e.g., water and metal), the actual read distance is reduced to 10 feet or less.

antenna, and packaging around the transponder, among other tag requirements. Passive tags can operate at low, high, ultrahigh, or microwave frequency (described in the next section). Examples of passive tag applications include mass transit passes, building access badges, and consumer products in the supply chain. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government and industry organizations.

Semipassive tags⁹ also do not initiate communication with the reader but contain batteries that allow the tag to perform other functions, such as monitoring environmental conditions and powering the tag's internal electronics. These tags do not actively transmit a signal to the reader. Some semipassive tags remain dormant (which conserves battery life) until they receive a signal from the reader. The battery is also used to facilitate information storage. Semipassive tags can be connected to sensors to store information for container security devices.

Active tags contain a power source and a transmitter, in addition to the antenna and chip, and send a continuous signal. These tags typically have read/write capabilities—tag data can be rewritten and/or modified. Active tags can initiate communication and communicate over longer distances—up to 750 feet, depending on the battery power. The relative expense of these tags makes them an option for use only where their high cost can be justified. Active tags are more expensive than passive, costing about \$20 or more per tag. Examples of active tag applications are toll passes, such as “E-Z pass,” and the in-transit visibility applications on major items and consolidated cargo moved by DOD.

Tags have various types of memory, including read-only, read-write, and write-once read-many. Read-only tags have minimal storage capacity (typically less than 64 bits) and contain permanently programmed data that cannot be altered. These tags primarily contain item identification information and have been used in libraries and video rental stores. Passive tags are typically read-only. In addition to storing data, read-write tags can allow the data to be updated when necessary. Consequently, they have larger memory capacity and are more expensive than read-only tags. These tags are typically used where data may need to be altered throughout a product's life cycle, such as in manufacturing or in supply chain

⁹Semipassive tags are also referred to as semiactive or battery-assisted passive tags.

management. A write-once, read-many tag allows information to be stored once, but does not allow subsequent alterations to the data. This tag provides the security features of a read-only tag while adding the additional functionality of read/write tags. The following table provides a summary of the characteristics of passive, semipassive, and active tags.

Table 1: Typical Characteristics of RFID Tags

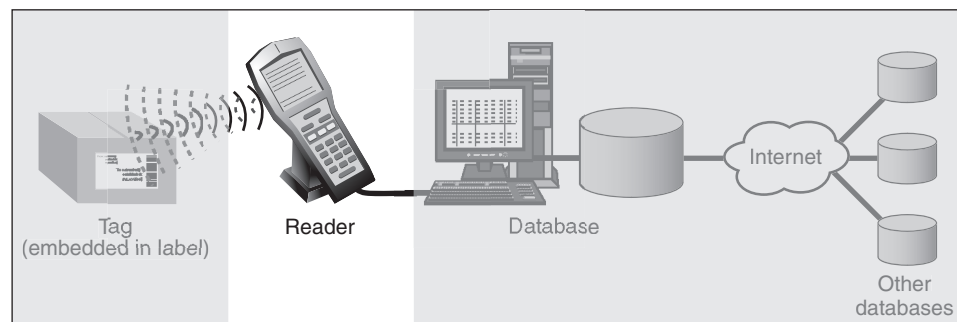
	Passive tags	Semipassive tags	Active tags
Power supply	external (from reader)	internal battery	internal battery
Read range	up to 20 feet	up to 100 feet	Up to 750 feet
Type of memory	mostly read-only	read-write	read-write
Cost	\$.20 to several dollars	\$2 to \$10	\$20 or more
Life of tag	up to 20 years	2 to 7 years	5 to 10 years

Source: National Institute of Standards and Technology and Robert W. Baird & Co., Inc., "RFID Explained: A Basic Overview" (February 2004).

The Reader

In order for an RFID system to function, it needs a reader, or scanning device, that is capable of reliably reading the tags and communicating the results to a database. (See fig. 3.)

Figure 3: The Reader



Source: GAO.

A reader uses its own antenna to communicate with the tag. When a reader broadcasts radio waves, all tags designated to respond to that frequency and within range will respond. A reader also has the capability to

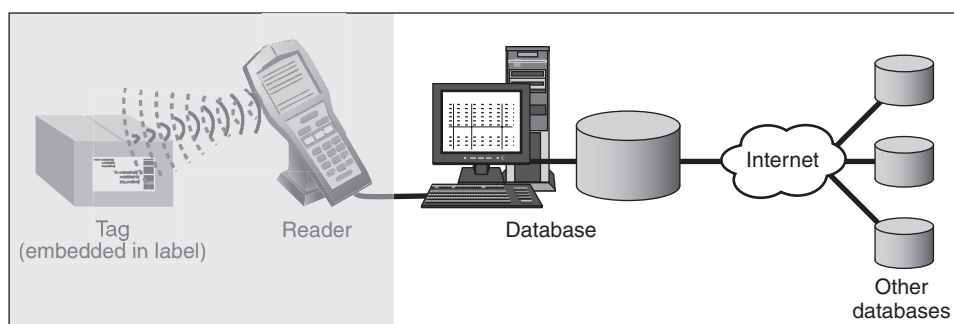
communicate with the tag without a direct line of sight, depending on the radio frequency and the type of tag (active, passive, or semipassive) used.

Readers can process multiple items at once, allowing for increased read processing times. They can be mobile, such as handheld devices that scan objects like pallets and cases, or stationary, such as point-of-sale devices used in supermarkets. Readers are differentiated by their storage capacity, processing capability, and the frequencies they can read.

The Database

The database is a back-end logistic information system that tracks and contains information about the tagged item. (See fig. 4.)

Figure 4: The Database



Source: GAO.

Information stored in the database can include item identifier, description, manufacturer, movement of the item, and location. The type of information housed in the database will vary by application. For instance, the data stored for a toll payment system will be different than the data stored for a supply chain. Databases can also be linked into other networks, such as the local area network, which can connect the database to the Internet. This connectivity can allow for data sharing beyond the local database from which the information was originally collected.

RFID Systems Operate on Radio Frequencies

Choice of radio frequency is a key operating characteristic of RFID systems. The frequency largely determines the speed of communication and the distance from which the tag can be read. Generally, higher frequencies indicate a longer read range. Certain applications are more suitable for one type of frequency than other types, because radio waves

behave differently at each of the frequencies. For instance, low-frequency waves can penetrate walls better than higher frequencies, but higher frequencies have faster data rates. In the United States, the Federal Communications Commission (FCC) administers the allocation of frequency bands for commercial use and the National Telecommunications and Information Administration (NTIA) manages the federal spectrum. RFID systems use an unlicensed frequency range, classified as industrial-scientific-medical or short-range devices, which is authorized by the FCC.¹⁰ Devices operating in this unlicensed bandwidth may not cause harmful interference and must accept any interference received. The FCC also regulates the specific power limit associated with each frequency. The combination of frequency and allowable power levels determine the functional range of a particular application, such as the power output of readers.

There are four main frequencies used for RFID systems: (1) low, (2) high, (3) ultrahigh, and (4) microwave.

Low-frequency bands range from 125 kilohertz (KHz) to 134 KHz. This band is most suitable for short-range use such as antitheft systems, animal identification, and automobile key-and-lock systems.

High-frequency bands operate at 13.56 megahertz (MHz). High frequency allows for greater accuracy within a 3-foot range, and thus, reduces the risk of incorrectly reading a tag. Consequently, it is more suitable for item-level reading. Passive 13.56 MHz tags can be read at a rate of 10 to 100 tags per second and at a range of 3 feet or less. High-frequency RFID tags are used for material tracking in libraries and bookstores, pallet tracking, building access control, airline baggage tracking, and apparel item tracking.

Ultrahigh-frequency tags operate around 900 MHz and can be read at longer distances than high-frequency tags, ranging from 3 to 15 feet. These tags, however, are more sensitive to environmental factors than tags that operate in other frequencies. The 900 MHz band is emerging as the preferred band for supply-chain applications due to its read rate and range. Passive ultrahigh-frequency tags can be read at about 100 to 1,000 tags per second, with efforts under way to increase this read rate. These tags are

¹⁰In the United States, the FCC authorizes the use of the 2.4 GHz and the 902-928 MHz frequency range for industrial-scientific-medical and short-range devices, which includes RFID technology.

commonly used in pallet and container tracking, truck and trailer tracking in shipping yards, and have been adopted by major retailers and DOD.

Additionally, in the United States, the 433 MHz band is used to identify the contents of shipping containers in commercial and industrial areas to allow timelier and more accurate data transmission. According to the FCC, such use could benefit commercial shippers and have significant homeland security benefits by enabling the entire contents of shipping containers to be easily and immediately identified, and by allowing a determination of whether the contents were tampered with during shipping.

Tags operating in the **microwave frequencies**, typically 2.45 and 5.8 gigahertz (GHz), experience more reflected radio waves from nearby objects, which can impede the reader's ability to communicate with the tag. Microwave RFID tags are typically used for supply chain management. Table 2 provides a summary of the operating frequencies for passive tags.¹¹

Table 2: Common RFID Operating Frequencies for Passive Tags

	Frequency	Typical read range and rate	Examples of use
Low frequency	125 KHz	~1.5 feet; low reading speed	Access control, animal tracking, point of sale applications
High frequency	13.56 MHz	~3 feet; medium reading speed	Access control, smart cards, item-level tracking
Ultrahigh frequency	860-930 MHz	up to 15 feet; high reading speed	Pallet tracking, supply chain management
Microwave frequency	2.45/5.8 GHz	~3 feet; high reading speed	Supply chain management

Source: National Institute of Standards and Technology and Bear Stearns, "Supply Chain Technology" (January 2004).

Further advancements in radio frequency technology and its applications are anticipated. Experts have suggested that the widespread implementation of these current research and development efforts is approximately 5 years away. Appendix II provides a discussion of these efforts.

¹¹The technology for tags, antennas, and readers is rapidly evolving, which may result in overlap between tag read distances in the near future.

Several Agencies Have Begun Implementation of RFID Systems

Within the federal government, the major initiatives at agencies that use or propose to use the technology include physical and logical access control and tracking various objects such as shipments, baggage on flights, documents, radioactive materials, evidence, weapons, and assets. Several agencies have initiated pilot programs to evaluate the use of RFID in specific applications. Of the 24 CFO Act agencies, 13 reported having implemented or having a specific plan to implement the technology in one or more applications. Table 3 provides a listing of the CFO Act agencies' reported uses of RFID technology. The remaining 11 agencies reported that they are not using the technology and do not have specific plans to implement it in the future.

Table 3: Federal Agencies' Reported Use or Planned Use of RFID Technology

Agency	Application
Department of Defense	Logistics support
	Tracking shipments
Department of Energy	Detection of prohibited articles
	Tracking the movement of materials
Department of Health and Human Services	Physical access control
Department of Homeland Security	Border control, immigration and customs (U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT))
	Location system
	Smart containers
	Tracking and identification of assets
	Tracking and identification for use in monitoring weapons
	Tracking and identification of baggage on flights
Department of Labor	Tracking and locating case files
Department of State	Electronic passport
Department of Transportation	Electronic screening
Department of the Treasury	Physical and logical access control
	Records management (tracking documents)
Department of Veterans Affairs	Audible prescription reading
	Tracking and routing carriers along conveyor lines
Environmental Protection Agency	Tracking radioactive materials
General Services Administration	Distribution process
	Identification of contents of shipments
	Tracking assets
	Tracking of evidence and artifacts
National Aeronautics and Space Administration	Hazardous material management
Social Security Administration	Warehouse management

Source: GAO analysis of agencies' survey responses.

Note: The Departments of Agriculture, Commerce, Education, Housing and Urban Development, Interior, and Justice; the U.S. Agency for International Development; the Nuclear Regulatory Commission; the National Science Foundation; the Office of Personnel Management; and the Small Business Administration reported no current use or specific plan to use RFID technology in either a pilot or an operational environment.

In addition to the initiatives reported by the 24 CFO Act agencies, other related federal initiatives are under way. While the U.S. Department of Agriculture reported that it is not using the technology and takes a technology-neutral stance, it noted that private-sector participants in its animal identification program have the option to use the technology to

track animals. Additionally, the General Services Administration is involved with procuring governmentwide contactless identification cards¹² in response to Homeland Security Presidential Directive 12.¹³ According to the General Services Administration, the card will not use RFID technology, but will use the International Organization for Standardization (ISO)¹⁴ and International Electrotechnical Commission¹⁵ (IEC) ISO/IEC 14443 standards for contactless technology.¹⁶

Another federal initiative is under way at the Food and Drug Administration. In February 2004, the agency published a report that promotes RFID technology to prevent counterfeit drugs. In November 2004, the agency stepped up its efforts by issuing a compliance policy guide to facilitate pilot projects that use the technology in the pharmaceutical sector. Accordingly, pharmaceutical companies are currently experimenting with RFID to prevent counterfeit drugs and to help improve drug quality from the manufacturer.

Multiple Sets of Standards Guide RFID Technology

RFID standards define a set of rules, conditions, or requirements that the components of a system (tag, reader, and database) must meet in order to operate effectively and that are needed to cover the air-interface operational requirements,¹⁷ ensure that tags meet intended designs,

¹²Contactless cards contain an embedded antenna and work when the card is waved within the magnetic field of a card reader or terminal. Contactless cards are better suited for environments where quick interaction between the card and reader is required, such as high-volume physical access.

¹³Homeland Security Presidential Directive 12/Hspd-12, August 27, 2004.

¹⁴ISO is a network of national standards institutes from 148 countries that works in partnership with international organizations, governments, industry, and business and consumer representatives to develop technical standards.

¹⁵IEC is a global body responsible for developing a consensus on global standards in the electrotechnical field.

¹⁶ISO/IEC 14443 standard is for proximity cards. It includes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for identification cards that operate within 10 centimeters (3.94 inches).

¹⁷Air-interface operational requirements are the parameters for interaction between a tag and the tag reader such as transmission and receiving frequencies and the algorithms by which the tag reader can communicate with the tag.

provide adequate protection of data for both security and privacy issues, and define coding information contained on the tags. Currently, multiple sets of standards guide the use of RFID technology. Additionally, multiple standards-setting organizations have developed standards that support these needs. These standards can vary based on the type of activity the application is used for and the industry or country in which it is used.

Multiple Organizations Develop RFID Standards

Multiple organizations, including international, national, private-sector, and industry organizations, are involved in the development of RFID standards. Appendix III contains an illustrative list of standards-setting organizations.

International standards-setting organizations generally develop standards through a process that is open to participation by representatives of all interested countries, transparent, consensus-based, and subject to due process. ISO and IEC are actively involved in developing RFID standards for international use. ISO is an international association of countries, each of which is represented by its leading standards-setting organization. The scope of ISO is broad and includes all fields except electrical and electronic standards, which are the responsibility of IEC. ISO and IEC have jointly created several RFID standards.

National standards-setting organizations facilitate the development of national standards for use within their country. For example, the American National Standards Institute (ANSI) represents the United States to ISO and facilitates the development of U.S. standards. ANSI, as well as other national standards organizations, is involved in the development of RFID standards. For example, the Standardization Administration of China has established a National RFID Standards Working Group to draft and develop a national standard.

Private-sector organizations involved in the development of RFID standards can represent a single industry or multiple industries. For example, the Automotive Industry Action Group, Universal Postal Union, and International Air Transport Association have developed RFID standards for their respective industries. Private-sector organizations that represent multiple industries can develop a standard for a specific application. For example, EPCglobal Incorporated, which partners with various industry groups, has developed a series of specifications that DOD and various private-sector users are implementing in their supply chains.

Separate Standards Have Been Developed for Specific Applications

The standards-setting organizations have developed separate sets of standards governing RFID systems for specific applications. The standards used often depend on the type of activity the application is used for and the industry or country in which it is used. Requirements of applications often differ, and a single, common set of standards may not meet the needs of all applications. Appendix IV contains an illustrative list of standards used for RFID systems.

RFID applications such as supply chain, animal tracking, and access control use separate standards because the needs of these applications differ. As previously mentioned, the frequency used affects the performance of tags in certain environments. For example, an animal tracking application will likely use a standard that specifies the use of the low-frequency range because this range performs well in environments that require reading through materials such as water and body tissue. An access control application that requires a read range of approximately 3 inches and the ability to read multiple tags simultaneously would likely use a standard that specifies the use of the high-frequency range. A supply chain application may likely use a standard that specifies the use of the ultrahigh-frequency range because this range provides a read range of up to 15 feet and a read rate of 100 to 1,000 tags per second.

Industries such as the automotive, postal, and aviation, use standards for industry-specific applications. They may use standards developed by industry standards-setting organizations or standards developed by other standards-setting organizations, such as ISO, IEC, and EPCglobal. For example, the aviation industry uses a standard created by an industry organization for identifying airplane parts by means of bar code and RFID technologies. This standard requires the use of an ISO standard for tracking parts.

There are also applications that only operate in a specific country. These applications, such as national identification cards, may be governed by national standards used only within that country.

Global Interoperability of RFID Systems May Require International Standards

For applications where global interoperability between systems is necessary, such as electronic passports or global supply chains, a common set of international standards can assist with proper interaction and interchange of information between systems. For example, global interoperability of machine-readable travel documents requires the use of a

common international standard. As previously mentioned, the U.S. Department of State has reported plans to use RFID technology in its electronic passports.¹⁸ The United States and other countries are anticipating using the International Civil Aviation Organization¹⁹ (ICAO) Document 9303 standard, which prescribes an international format for passports, visas, and other official machine-readable travel documents.

To maximize the global interoperability of supply chains using RFID technology, it is important to ensure that the standards chosen can be used in all relevant markets. Interoperability of global supply chains using RFID technology means that tags used in one country can be read easily by readers in other countries. ISO's item management standard for frequency interoperability includes its ISO 18000 series. This series addresses issues such as generic air interface parameters for globally accepted frequencies and air interface communications parameters at different operating frequencies. To complement ISO's standard, EPCglobal has proposed its Generation 2 standard. EPCglobal claims that this standard will allow for global interoperability of systems built to it for supply chain management because frequency and power level used within this standard comply with most relevant markets.²⁰ As previously mentioned, DOD and various private-sector organizations are currently using EPCglobal's specifications in their supply chains; the specifications cover issues such as placement of the tag, structure of the coding for the tag, specifications for tag data, and parameters for interaction between a tag and a reader.

Federal Agencies Raise Few Legal Issues

Of the 16 agencies that responded to the question on legal issues associated with RFID implementation in our survey, only one identified what it considered to be legal issues. These issues relate to protecting an individual's right to privacy and tracking sensitive documents and

¹⁸The proposed U.S. electronic passport will resemble a regular passport with the addition of a small RFID chip embedded in the back cover. The chip will securely store the same data visually displayed on the photo page of the passport and will also include a digital photograph.

¹⁹ICAO was chartered by the United Nations to regulate international aviation and includes the United States and 188 other nations.

²⁰Each country makes its own allocations of spectrum use; therefore, allocation decisions may differ in other regions of the world and in other countries. Additionally, the allowable power for RFID devices is not generally the same from region to region.

evidence. The remaining 15 agencies that responded did not raise legal issues associated with RFID implementation.

Security and Privacy Considerations with RFID

Several security and privacy issues exist that are related to federal and commercial use of RFID technology. The security of tags and databases raises important considerations concerning the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Measures to address these security issues, such as compliance with the risk-based framework mandated by FISMA and employing encryption and authentication technologies, can help agencies achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes or predilections; and allowing for secondary uses of information. While measures to mitigate these issues are under discussion, they remain largely prospective.

Security Considerations Relate to Data Confidentiality, Integrity, and Availability

Several agencies identified data confidentiality, integrity, and availability as key security considerations with implementing RFID technology. Thirteen agencies reported having implemented or having a specific plan to implement RFID technology. Six of the 13 identified security considerations. Specifically, these issues included ensuring that only authorized readers or personnel have access to information, maintaining the integrity of the data on the chip and stored in the databases, and ensuring that critical data is fully available when necessary. Other issues with implementing the technology included the potential for various attacks, such as counterfeiting or cloning,²¹ replay,²² and eavesdropping; the possibility of electronic collisions when multiple tags and/or readers are present; and the presence of unauthorized components that may interfere or imitate legitimate system components.

²¹Cloning an RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.

²²A replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it.

Without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users.

Practices and Tools in Place to Address Security Considerations

Using security practices and tools such as the risk-based framework mandated by FISMA, encryption, and authentication can help mitigate the security considerations associated with implementing RFID technology.

Implementing the security practices required in FISMA can help strengthen the security of RFID systems that store information transmitted from tags. FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk but no less than annually, and which includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

-
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
 - procedures for detecting, reporting, and responding to security incidents; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Encrypting the data on the tags, in the air, or stored in a database may also reduce the risk of unauthorized use or changes. Using encryption may be particularly relevant for applications where sensitive information is contained on the tag. Encryption is the process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) using a special value known as a key and a mathematical process called an algorithm. Cryptographic algorithms are designed to produce ciphertext that is unintelligible to unauthorized users. Decryption of ciphertext is possible by using the proper key. Encryption technologies can be used to (1) hide information content, (2) prevent undetected modification, and (3) prevent unauthorized use. When properly implemented, encryption technologies may provide assurance regarding the confidentiality, integrity, or origin of information that has been exchanged. It may also provide a method by which the authenticity can be confirmed. Without strong encryption, the data may not be kept confidential. For instance, an RFID chip that used a 40-bit key and a confidential cipher was successfully reverse-engineered, thereby allowing the data to be decrypted. One agency reported that its use of encryption as part of its security measures has helped to prevent unauthorized interception of communication.

Authentication, which is the process of verifying the claimed identity of a user, can be used between tag and reader as a way to mitigate security risks. Authentication of readers can help prevent the unauthorized reading and/or writing to tags.

Privacy Issues Surrounding RFID Use

The extent and nature of the privacy issues related to the federal and commercial use depends on the specific proposed use. For example, using the technology for generic inventory control would not likely generate substantial privacy concerns. However, the use of RFIDs by the federal government to track the movement of individuals traveling within the United States could generate concern by the affected parties. Privacy

issues associated with RFID implementation include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of information.

- **Notification.** Individuals may not be aware that the technology is being used unless they are informed that the devices are in use. Therefore, unless they are notified, consumers may not be aware that the RFID tags are attached to or embedded in items they are browsing or purchasing or that the items purchased are being scanned.
- **Tracking.** Tracking is real-time, or near-real-time, surveillance in which a person's movements are followed through RFID scanning. Media reports have described concerns about ways in which anonymity is likely to be undermined by surveillance. As previously reported, many civil liberties groups are concerned about the application of this technology to track individuals' movements, such as in a public school setting, and the resulting loss of anonymity in public places. Additionally, periodic public surveys have revealed a distinct unease with the potential ability of the federal government to monitor individuals' movements and transactions.²³ Three agencies also indicated that employing the technology would allow for the tracking of employees' movements.
- **Profiling.** Profiling is the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections. Because tags can contain unique identifiers, once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual. As previously reported,²⁴ profiling for race, ethnicity, or national origin has caused public debate in recent years. Both tracking and profiling can compromise an individual's privacy and anonymity.
- **Secondary uses.** In addition to issues about the planned uses of such information, there is also concern surrounding the possibility that

²³GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 15, 2002).

²⁴[GAO-03-174](#).

organizations could develop secondary uses for the information; that is, information collected for one purpose tends over time to be used for other purposes as well. This has been referred to as “mission-” or “function-creep.” The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.²⁵ Secondary uses of the Social Security number have been a matter not of technical controls but rather of changing policy and administrative priorities.

The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated. As the uses of technology proliferate, consumers have raised concerns about whether certain collected data might reveal personal information such as medical predispositions or personal health histories and that the use of this information could result in denial of insurance coverage or employment to the individual. For example, the use of RFID technology to track over-the-counter or prescription medicines has generated substantial controversy. Additionally, three agencies raised the issue of protecting personal data, such as date of birth and biometrics, contained on the tag as well as the associated database that stores this information.

Practices and Tools to Mitigate Privacy Issues Are in Progress

Implementing privacy practices and tools, such as existing requirements contained in the Privacy Act of 1974 and the E-Government Act of 2002, and employing proposed measures such as a deactivation mechanism on the tag, blocking technology to disrupt transmission, and an opt-in/opt-out framework for consumers can help mitigate some of these privacy issues. While these proposed techniques may address some of the privacy issues, they are largely prospective in nature.

An existing legal framework that addresses the privacy issues under which federal agencies operate when implementing any new information technology is defined in the Privacy Act of 1974, which limits federal

²⁵GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, [GAO-02-352](#) (Washington, D.C.: May 31, 2002).

agencies' use and disclosure of personal information. The act's protections are keyed to the retrieval of personal information by a "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."²⁶ The Privacy Act generally covers federal agency use of personal information, regardless of the technology used to gather it. As a practical matter, however, the Privacy Act is likely to have a limited application to the implementation of RFID technology because the act only applies to the information once it is collected, not to whether or how to collect it. The E-Government Act's privacy impact assessments requirement, however, provides a means of evaluating whether or not to collect information based on privacy concerns.

Employing a mechanism that can deactivate, or "kill," a tag at the point of sale, can prevent tracking of the individual and item once the tag leaves a store. This feature would still provide the supply chain tracking benefits to the retailer without providing additional information about the consumer beyond the point of sale. However, enforcement may be a challenge, as a tag may inadvertently be deactivated or remain dormant with the potential to be reactivated. Additionally, consumers opting to have the tags deactivated may have to undergo additional procedures that may cost time or money.

Another proposed method is blocking technology. Devices that can disrupt the transmission of all or selected information contained on a tag would be embedded in an object that is carried or worn near RFID tags that the individual wants blocked. This technology, however, has not yet been fully developed. One challenge to its development may be the constant proximity required between the blocker tag and the tag in order to disrupt data transmission. Consumers may not consistently remember to juxtapose the tags, thereby reducing the effectiveness of the technology. A physical method of blocking currently in use is aluminum-coated Mylar²⁷ bags, which can absorb or diffuse RFID signals when placed over the tag. An example is in toll payment systems where aluminum-coated Mylar bags are issued along with the tag so that drivers can place their tags in the bag to prevent them from being read inadvertently. Additionally, the State

²⁶5 U.S.C. § 552a(a)(4).

²⁷Mylar is a registered trademark of Dupont Tejin Films that generally refers to plastic film. A common application is packaging film for food, electronics, and medical devices.

Department is reported to have plans to include metal inside U.S. passport jackets to help prevent the chip from being read by anyone except customs and border agents.

Government and industry groups have also proposed using an opt-in/opt-out framework. This framework would provide consumers with an option to voluntarily participate in RFID transactions that gather data about them. Consumers would be informed of the existence of the tags and the type of information that would be collected and could then decide whether to participate in the transaction or opt out. A concern of this hybrid system is the potential disparity in benefits received between consumers who opt in versus those who opt out, similar to customer loyalty cards, and the notion that this framework might penalize consumers who articulate their privacy preferences. Also, a study by the RAND Corporation has suggested that organizations using RFID workplace access devices should implement “fair information practices” and communicate those policies to employees.²⁸

The Federal Trade Commission, following research and consumer input at a workshop it sponsored, announced in a March 2005 report that it would, for the time being, allow companies that make and use the technology to regulate themselves regarding consumer privacy. The Federal Trade Commission report noted, however, that “many of the potential privacy issues associated with RFID are inextricably linked to database security. As in other contexts in which personal information is collected from consumers, a company that uses RFID to collect such information must implement reasonable and appropriate measures to protect that data.”²⁹

Other Areas of Consideration Are Relevant to RFID Adoption

In addition to privacy and security, other areas of consideration related to the adoption of RFID technology include the reliability of tags and readers, the placement of the tags, the costs and benefits of implementation, the availability of tags, and environmental issues.

Reliability. Currently, tags are not always reliable and will not work with some products or in certain situations. When something close to the reader

²⁸The RAND Corporation, *Privacy in the Workplace: Case Studies on the Use of Radio Frequency Identification in Access Cards*, RB-9107-RC (Santa Monica, Calif.: 2005).

²⁹Federal Trade Commission, *Radio Frequency Identification: Applications and Implications for Consumers* (Washington, D.C.: March 2005).

or tag interferes with the radio waves, read-rate accuracy decreases. For instance, defective tags created by the manufacturer can be unreadable or tags may be damaged during the supply chain process. Additionally, readers can produce false negatives (a reader does not read a valid tag that passes within the prescribed range) or false positives (a tag not intended to be read inadvertently passes within range of a reader), which typically occur with closely packed items where multiple tags are near each other. Further, environmental conditions, such as temperature and humidity, can make tags unreadable. Experts have indicated that tags read at high speeds have a significant decrease in read rate. As the technology continues to mature, these limitations may eventually be addressed, but currently they remain a challenge to organizations. One agency official reported not implementing the technology because its reliability was not at an acceptable level.

Placement. The placement and orientation of the tag contributes to how effectively the reader can scan it. Factors to consider in tag placement are read and nonread points on objects such as items, cases, or pallets; locations that minimize the risk of damage to the tag and have the highest potential for a successful passive tag reading; and read points in specific environments, such as an item running through a conveyor belt at various speeds.

Some organizations, such as DOD, have documented procedures for tag placement to help ensure placement precision, consistency, and efficiency. Determining optimal tag placement may require software or an automated application to improve this otherwise manual process.

Costs and Benefits. Best practices for information technology investment dictate that prior to making any significant project investment, the costs and benefits of the system should be analyzed and assessed in detail.³⁰ The cost of the tags generally falls on the supplier, as it is the supplier who tags the items. Retailers see benefits from RFID tags such as improved product visibility during the supply chain process. Suppliers can also see such benefits when they go beyond the “slap and ship”³¹ model and find new

³⁰GAO, *Aviation Security: Challenges in Using Biometric Technologies*, [GAO-04-785T](#) (Washington, D.C.: May 19, 2004).

³¹“Slap and ship” is when a supplier tags the products with an RFID tag right before shipping them to the retailer. Suppliers who slap and ship generally will not benefit from the technology because they do not make use of it for their own benefit.

ways to make the technology add value to gain a return on investment. According to the National Institute of Standards and Technology, smaller suppliers may earn little to no return because the costs associated with implementing the technology, such as hardware, software, infrastructure, middleware,³² and training will be a substantial portion of a small supplier's budget. Additionally, their price per-tag may be high since they do not order large quantities. Organizations need to determine if the cost of implementing this technology, which is still in the early stages of adoption, is worth the increased ability to collect and analyze data.

Availability. With increasing adoption of RFID technology, the availability of tags may emerge as a growing concern. The increased adoption of the technology will result in greater demand for tags. As a result, the demand for tags may eventually outstrip the supply. Even if industry can keep up with the demand, damage to the tags during production may create a shortage. For instance, according to a research group's survey of RFID vendors, up to 30 percent of chips are damaged during production when they are attached to their antennae, and an additional 10 to 15 percent are damaged during the printing process. Improving tag manufacturing and quality control processes may help increase the availability of operative tags.

Environment. In September 2004, the Environmental Protection Agency (EPA) and the Office of the Federal Environmental Executive (OFEE) cohosted a workshop on the impact of tags on the reuse and recycling of packaging materials. Tags contain silicon, adhesives, and nickel, and the antennae are typically made from copper, aluminum, or, if printed, silver. According to OFEE, these elements of the tags are potential contaminants for recyclers and manufacturers using recycled materials. As such, OFEE and EPA believe that it is essential that these industries begin to understand the potential impacts of having tags on packaging materials and pallets and plan how to minimize the impact on the environment. One manufacturer remarked on the lack of practicality in recycling because of the small amount of silicon used in the chip. Currently, EPA does not provide clear national guidelines on electronic waste (e-waste) disposal nor has it defined its e-waste goals and measures. Consequently, states are pursuing their own mechanisms to regulate e-waste. According to one agency official, proper disposal of a tag, including reuse and recycling, remains a challenge. As tagging begins to include cases, additional

³²Middleware is software that connects two otherwise separate applications.

environmental issues may arise because cases are not reusable, in contrast to the pallets, which are reusable.

Summary

RFID technology can provide new capabilities as well as an efficient method for federal agencies, manufacturers, retailers, and other organizations to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls by providing real-time access to information. Several federal agencies have already begun testing and using the technology for access control and tracking and tracing assets and documents.

Because various standards exist based on the application and the industry or country in which it is used, interoperability may also be a factor to consider, although a single, common set of standards may not be necessary among different applications.

Few legal issues associated with RFID implementation were raised by the agencies. The use of the technology, however, raises several security and privacy considerations that may affect federal agencies' decisions to implement the technology. Key security issues include protecting the confidentiality, integrity, and availability of the data and information systems. The privacy issues include notifying consumers; tracking an individual's movements; profiling an individual's habits, tastes, and predilections; and allowing for secondary uses of information. In addition, other areas such as the reliability, placement, and availability of tags, along with the cost and benefits of implementation and environmental concerns, are factors to consider. As agencies continue to deliberate over implementation, the considerations we identified are among the key factors to address.

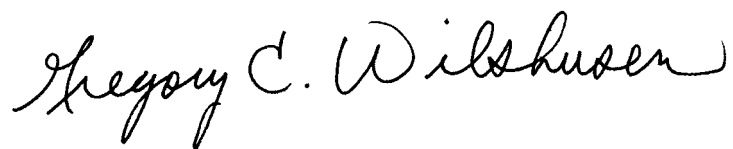
Agency Comments

In providing comments via e-mail on a draft of this report, representatives of the Office of Management and Budget's Office of Information and Regulatory Affairs and Office of General Counsel stated that they agreed with the contents of the report. They also provided technical comments that we addressed in the report, as appropriate.

We are sending copies of this report to interested congressional committees. We will also provide copies to others on request. In addition,

the report will be made available at no charge on GAO's Web site at <http://www.gao.gov>.

If you have any questions concerning this report, please call me at (202) 512-6244 or send an e-mail to wilshuseng@gao.gov. Key contributors to this report are included in appendix V.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive, flowing style.

Gregory C. Wilshusen
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to (1) provide an overview of the technology, with an emphasis on passive technology; (2) identify the major initiatives at federal agencies that use or propose to use the technology; (3) discuss the current standards, including those for interoperability, that exist; (4) discuss potential legal issues that the 24 Chief Financial Officer (CFO) Act agencies have identified in their planning for technology implementation; and (5) discuss security and privacy considerations surrounding the technology and the tools and practices available to mitigate them.

To provide an overview of the technology, we analyzed research studies and reports discussing the technology and its application. We also conducted an extensive Internet search of professional information security literature produced by information security experts, practitioners, and news organizations. To identify the major initiatives that federal agencies use or propose to use RFID technology for and their concerns, we sent a questionnaire to 23 of the 24 executive branch agencies covered by the CFO Act of 1990. The Department of Defense was not issued a survey because relevant data were collected through other ongoing work we are performing. All 23 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documents that agencies provided to help verify their responses. We contacted agency officials when necessary to clarify their responses or to obtain additional information about their use or proposed use of RFID technology. We then analyzed agency responses to determine the extent to which agencies are using or proposing to use RFID technology. In addition, we analyzed their responses concerning security, privacy, legal, and other issues related to RFID. We also reviewed prior reports and testimonies on information security that discussed privacy and security issues.

To discuss the current standards, we met with leading standards-setting organizations, the National Academy of Sciences, and the National Institute of Standards and Technology to discuss the standards used, the various standards-setting organizations, and the current state of standards. We also reviewed relevant literature, research studies, and reports.

To discuss the potential legal issues agencies identified in planning for technology implementation, we analyzed agencies' survey responses and reviewed relevant reports. We also assessed relevant legal issues associated with the implementation of new information technology such as RFID.

Finally, to discuss the security and privacy considerations and the practices and tools available to mitigate them, we contacted the agencies and met with commercial suppliers, public interest groups, system integrators, academics, and users to discuss their experiences with or concerns related to the development and implementation of the technology. We also interviewed scientists and experts from the National Academy of Sciences, the National Institute of Standards and Technology, the National Telecommunications and Information Administration, and the Federal Trade Commission to discuss their current efforts, concerns, and expert opinions on RFID technology and its applications. Further, we analyzed their responses and related documents provided to identify the key security and privacy concerns associated with RFID implementation. Lastly, we analyzed relevant legislation, reviewed prior reports, and evaluated proposed measures to identify practices and tools available to mitigate these issues. We performed our review in Washington, D.C., from September 2004 through April 2005 in accordance with generally accepted government auditing standards.

Research and Development Efforts Are Under Way

Further advancements in radio frequency technology and its applications are anticipated. Some of these efforts include the development of organic tags, reversed mobility of tags and readers, and embedded systems. Experts have suggested that the widespread implementation of these current research and development efforts is approximately 5 years away.

Organic Tags

Efforts are in progress to make printable RFID tags from organic or carbon-based materials. This alternative may include printing tags (including the antenna and chip) from carbon-based plastics. Proponents claim that organic tags may eventually cost as little as 1 cent per tag, thereby making item-level tagging more feasible. Organic tags, however, may not be as powerful nor have as much data storage space as tags with silicon chips. These tags are projected to operate at the 13.56 MHz (high-frequency) band.

Reversed Mobility of Tags and Readers

Research is also under way to reverse the mobility of the tags and readers so that the tags are stationary and the readers move. For example, a security guard performing a routine perimeter check could scan a stationary tag, located at each door, with a mobile reader to confirm that the door is secured. The reader would transmit this information to a central database, or control center, allowing for real-time monitoring of the guard's status. This reversed functionality is being tested in the energy, gas supply, and security industries. This usage could also be helpful to first responders by providing reliable tracking of first responders in environments when other technologies, such as global positioning systems, are known to be unreliable. Additionally, critical building and occupant information in specific on-site RFID tags has the potential to enhance the safety and efficiency of the missions of first responders, as well as minimize dependence on communication with other external systems.

Embedded Systems

An embedded system is a special-purpose computer system that is used within a device. An embedded system has specific requirements and performs predefined tasks, unlike a general-purpose personal computer. To date, embedded RFID chips have been tested in "smart" test tubes that store data about the tube's contents, which has facilitated obtaining correct information for identifying specimens and time-stamping doctor's orders. Embedded chips in credit cards and mobile phones for contactless

Appendix II
Research and Development Efforts Are
Under Way

payments¹ are also expected to become increasingly popular in Asia. Embedded RFID chips are being proposed for use in numerous applications, including electronic passports, tires to determine wear, drug containers for tracking and theft control, and aircraft for maintenance.

¹Contactless payments are noncash transactions where there is no physical connection between the consumer's payment device and the point-of-sale terminal.

Illustrative List of Standards-Setting Organizations for RFID Systems

Type of standards body	Organization	Description
International	International Organization for Standardization (ISO)	A network of national standards institutes from 148 countries that works in partnership with international organizations, governments, industry, and business and consumer representatives to develop technical standards.
International	International Electrotechnical Commission (IEC)	Produces international standards for electrical, electronic, and related technologies. Its members include manufacturers, providers, distributors, vendors, consumers, users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries.
International	International Civil Aviation Organization (ICAO)	Chartered by the United Nations to regulate international aviation and includes the United States and 188 other nations.
International—professional	Institute of Electrical and Electronics Engineers (IEEE)	With more than 360,000 members in approximately 175 countries, the organization, through its members, works in the technical areas ranging from aerospace, computers, and telecommunications to biomedicine, electric power, and consumer electronics.
Regional	Comité Européen de Normalisation (CEN)	Contributing to the objectives of the European Union and European Economic Area with voluntary technical standards.
Regional	European Telecommunications Standards Institute (ETSI)	Produces standards for telecommunications, broadcasting, and related areas, such as intelligent transportation and medical electronics.
National	American National Standards Institute (ANSI)	Promotes and facilitates voluntary consensus standards and conformity assessment systems and safeguards their integrity.
National	British Standards Institute (BSI)	Works with government, businesses, and consumers to represent the United Kingdom's interests and facilitate the production of British, European, and international standards.
National	Japanese Industrial Standards Committee (JISC)	Consists of many national committees and plays a central role in standardization activities in Japan.
National	Standardization Administration of China (SAC)	Authorized to exercise the administrative functions and carry out centralized administration for standardization in China.
Private sector	AIM Global	Working with its members, AIM Global develops standards and practices for automatic identification and data collection technologies.
Private sector	EPCglobal, Inc.	A joint venture between EAN International and the Uniform Code Council. Its subscribers include manufacturers, retailers, wholesalers, carriers, government, hardware and software companies, consultants, systems integrators, and training companies. EPCglobal has developed a series of specifications for use in the supply chain.
Industry	Automotive Industry Action Group (AIAG)	With more than 1,600 member companies which include North American, European and Asia-Pacific OEMs and suppliers to the automotive industry, the organization developed standards for use in the automotive industry and its goals include reducing cost and complexity within the automotive supply chain.
Industry	International Air Transport Association (IATA)	It is an inter-airline cooperation in promoting safe, reliable, secure, and economical air services - for the benefit of the world's consumers. It has over 270 members from more than 140 nations.

Appendix III
Illustrative List of Standards-Setting
Organizations for RFID Systems

(Continued From Previous Page)

Type of standards body	Organization	Description
Industry	Universal Postal Union (UPU)	With 190 member countries, it is a specialized agency of the United Nations that governs international postal service.

Source: GAO analysis of standards-setting organizations.

Illustrative List of Standards for RFID Systems

Standard	Application	Description	Frequency
ISO/IEC 14443	Identification cards	ISO/IEC standard for proximity cards. It includes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for identification cards that operate within 10 centimeters (3.94 inches).	13.56 MHz
ISO/IEC 15693	Identification cards	ISO/IEC standard for vicinity cards. It includes standards for the physical characteristics, radio frequency power and signal interface, and anticollision and transmission protocol for identification cards that operate within 1 meter (approximately 3.3 feet).	13.56 MHz
ISO 11784/11785	Identification of animals	ISO 11784 defines the code structure for the identification of animals. ISO 11785 defines the technical concept of the reader-tag communication for the identification of animals.	134.2 KHz
ISO 17363 DRAFT	Item management (freight containers)	ISO standard for supply chain applications regarding freight containers.	433 MHz
ISO/IEC 18000	Item management	An ISO/IEC standard for the air interface.	
		• Part 2	Below 135 KHz
		• Part 3	13.56 MHz
		• Part 4	2.45 GHz
		• Part 6	860-960 MHz
		• Part 7	433 MHz
ISO/IEC TR24729-2	Recycling	ISO/IEC implementation guidelines for recycling RFID tags.	Not applicable
EPC Version 1.0/1.1 Specifications	Supply Chain	EPCglobal Incorporated specification that defines the physical placement of the tag, tag-coding structure, and tag data specification.	
		• 900 MHz Class 0 RFID Tag Specification	900 MHz
		• 860 MHz-930 MHz Class 1 RFID Tag Radio Frequency and Logical Communication Interface Specification	860-930 MHz
AIAG B-11	Tire and wheel identification	Automotive Industry Action Group standard for tire and wheel identification.	862-928 MHz; 2.45 GHz

Source: GAO analysis of existing RFID standards.

Staff Acknowledgments

Staff Acknowledgments

Nicole Carpenter, Nancy Glover, Min Hyun, Carol Langelier, Stephanie Lee, Suzanne Lightman, and Charles Roney made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548